REMARKS

Prior to entry of the instant amendment, claims 17-33 were pending in the subject application. By this Amendment, claims 17, 18, and 20-33 are amended, claim 19 is canceled without prejudice to or disclaimer of the subject matter contained therein; and claims 33-36 are added. No new matter is added. Claim 17 is the sole independent claim.

Claims 17, 18, and 20-36 are presented to the Examiner for further or initial prosecution on the merits.

Favorable reconsideration of this application, in light of the preceding amendments and following remarks, is respectfully requested.

Applicants note with appreciation the Examiner's acknowledgement that certified copies of all priority documents have been received by the U.S.P.T.O.

Applicants also appreciate the Examiner's indication that the Information Disclosure Statement filed on January 18, 2005, has been considered.

Applicants also respectfully note the present action indicates that the drawings have been accepted by the Examiner.

Objections to the Specification

1) The disclosure is objected to because the layout of the specification is not clear, i.e., the location of background, summary, and the detailed description.

By this amendment, the specification has been amended to include section headings. Withdrawal of the objection is respectfully requested.

2) The Abstract of the disclosure is objected to due to informalities.

The Abstract has been amended and replaced at the end of this amendment, taking into consideration the Examiner's comments, to obviate the objection. Withdrawal of the objection is respectfully requested.

Objections to the Claims

Claims 17, 18, 21, 24, 27 and 30-33 are objected to due to informalities. By this amendment, Applicants have amended claims 17, 18, 21, 24, 27 and 30-33, taking into consideration the Examiner's comments, to obviate the objections. Applicants, however, note that claims 24 and 33 are not duplicate claims because claim 24 depends directly from claim **"22"** and claim 33 depends directly from claim **"23"**. Due to the different claim dependency, claims 24 and 33 are not duplicate claims.

Accordingly, reconsideration and withdrawal of the objections to the claims are respectfully requested.

Claim Rejections - 35 U.S.C. § 112

Claim 21 is rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicants regard as the invention. Applicants respectfully traverse this rejection for the reasons discussed below.

Applicants have amended claim 21 to recite that "the broadcasting device generates at least two test keys and transmits the at least two test keys to the processing device, received from the processing device the corresponding cryptograms, selects one control cryptogram from the list of control data and the associated test key for the verification operations and another control cryptogram and the associated test

key as session key for the encryption of the data encryption." Since claim 21 now positively recite that the processing device sends the cryptograms and associated test keys, it is clear and definite.

Accordingly, reconsideration and withdrawal of the objections to the claims are respectfully requested.

Claim Rejections - 35 U.S.C. § 102

Claims 17, 25-27 and 30 are rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 6,038,321 ("Torigai"). Applicants respectfully traverse this rejection for the reasons discussed below.

Applicants respectfully submit that the Torigai reference fails to disclose or suggest each and every element of claim 17, and therefore, an anticipatory rejection has not been established.[1]

For example, claim 17, as amended, recites, *inter alia*:

> determining the validity of the network key by comparing the received cryptogram with at least one of a plurality of control cryptograms taken from a list of control data generated by a verification center for the test key.

In particular, Applicants respectfully submit that the Torigai reference fails to disclose or suggest, *comparing the received cryptogram with control cryptograms taken from a list of control data generated by a verification center for the test key*, as recited in amended claim 17.

The Torigai reference, on the other hand, discloses on *col. 10, lines 31-58* that:

[1] A claim is anticipated only if each and every element as forth in the claim is found, either expressly or inherently described, in a single prior art reference. See MPEP § 2131; *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987).

> .....Subsequently, at step S205, in the member terminal T, the card interface section 61 encrypts the received challenge code CC using a private net-key SK stored in the loaded IC card C1, and sends back the encrypted challenge code CC as a response code RC to the member administrative server S. Then, at step S206, in the member administrative server S, the authenticating section 36 performs the final user authentication. Specifically, the authenticating section 36 decodes the received response code RC using a private net-key SK of the corresponding member stored in the member data administrative device 5 to derive a challenge code CC and checks whether the thus derived challenge code CC matches the foregoing challenge code CC held in the authenticating section 36.....

In other words, based on the above, the Torigai reference discloses a standard scheme in which a random number CC is sent to a card C1. The card C1 encrypts the code CC using a secret key SK and returns it to the server S. It is the server S that recognizes the secret key SK and, therefore, decrypts the cryptogram to extract the code CC. Accordingly, the Torigai reference teaches that the comparison is made between the decrypted CC and the initially generated code CC. That is, the server S in Torigai identifies the secret key SK for decrypting the encrypted random number returned by the receiver in order to compare the decrypted random number with the previously generated random number.

In contrast, the claimed invention may be carried out in a case that the server has no access to the secret key, e.g., a third party having authority may issue a list of cryptograms as well as their corresponding test keys for verification. The list may be transferred to the broadcasting device for further verification. Hence, it is noted that at no time, the network keys are stored in the broadcast device. Accordingly, in order to verify a network key, without having the network key itself, the broadcasting device sends a test key to the processing device. The processing device responds with a cryptogram, i.e., a test key encrypted by its network key. The broadcasting device can then compare the received cryptogram with the expected cryptogram received

previously by the authority. Therefore, the indirect verifying validity of the network key by the cryptograms provided by an authority is not disclosed in the Togirai reference. Again, it is the server that recognizes the secret key and is able to decrypt the cryptograms to extract the random number. The comparison is therefore made between the decrypted random number and the initially generated one.

To further illustrate Applicants' invention, FIG. 2 illustrates a communication initialization method according to an example, non-limiting embodiment, that replaces a session key (SK), in a first phase, by a test key (TK). For this, the decoder (e.g., the broadcasting device) has at its disposal a control list $\{(TK)_{NK1}, (TK)_{NK2}, (TK)_{NK3} \ldots\}$ of cryptograms and a test key. For example:

1) The terminal module (CT) of the first device may transmit its public key (PK) to the converter module (CC) of the decoder (STB).

2) The converter module (CC) (e.g., the broadcasting device) may have at its disposal a control list $\{(TK)_{NK1}, (TK)_{NK2}, (TK)_{NK3} \ldots\}$ as well as a test key (TK). The converter module (CC) may encrypt the test key (TK) with the public key (PK) received from the terminal module (CT), which may give a new message $(TK)_{PK}$ that will be retransmitted to the terminal module (CT).

3) The terminal module (CT) may decrypt the test key (TK) using its private key associated to the public key (PK). It then may encrypt the test key (TK) by means of the network key (NK) that it stores permanently. The resulting cryptogram $(TK)_{NK}$ may be transmitted to the converter module (CC).

4) The converter module may compare the cryptogram constituting the test key encrypted by the network key $(TK)_{NK}$ with those indexed in the control list $\{(TK)_{NK1}, (TK)_{NK2}, (TK)_{NK3} \ldots\}$ that can be either a black list that is a list of the unauthorized values, or a white list that is a list of the authorized values.

5) The terminal module (CT) may decrypt the session key (SK) using its private key linked to the public key (PK). It may then encrypt the session key (SK) by means of the network key (NK) that it stores permanently. The resulting message $(SK)_{NK}$ may be transmitted to the converter module (CC).

Therefore, the control list $\{(TK)_{NK1}, (TK)_{NK2}, (TK)_{NK3} \ldots\}$ may be stored in the decoder memory after reception because it can constitute a file that is too large to be stored in a converter module (CC). The comparison of the cryptogram $(TK)_{NK}$ with the contents in the list $\{(TK)_{NK1}, (TK)_{NK2}, (TK)_{NK3} \ldots\}$ may be carried out by the decoder (STB).

Accordingly, Applicants respectfully submit that the Torigai reference fails to disclose or suggest, *at least*, "determining the validity of the network key by comparing the received cryptogram with at least one of a plurality of control cryptograms taken from a list of control data generated by a verification center for the test key," as recited in amended claim 17.

Since the Torigai reference fails to disclose each and every element of claim 17, it cannot provide a basis for a rejection under 35 U.S.C. § 102(b) and, thus, is allowable. Claims 25-27 and 30 depend from amended claim 17 and, therefore, allowable for the similar reasons discussed above with respect to claim 17.

For at least these reasons, the Examiner is respectfully requested to reconsider and withdraw the § 102(b) rejection of claims 17, 25-27 and 30.

Claim Rejections - 35 U.S.C. § 103

Claims 18-21, 23, 24, 28 and 31-33 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Torigai in view of U.S. Patent No. 7,237,108 ("Medvinsky"). Applicants respectfully traverse this rejection for the reasons discussed below.

Claims 18-21, 23, 24, 28 and 31-33 are believed to be allowable for at least the reasons set forth above regarding claim 17. The Medvinsky reference fails to provide the teachings noted above as missing from the Torigai reference. Since claims 18-21, 23, 24, 28 and 31-33 are patentable at least by virtue of their dependency on

independent claim 17, Applicants respectfully request that the rejection of claims 18-21, 23, 24, 28 and 31-33 under 35 U.S.C. § 103(a) be withdrawn.

Claim 22 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Torigai in view of Medvinsky further in view of U.S. Patent No. 6,925,562 ("Gulcu"). Applicants respectfully traverse this rejection for the reasons discussed below.

Claim 22 is believed to be allowable for at least the reasons set forth above regarding claim 17. The Gulcu reference fails to provide the teachings noted above as missing from the Torigai reference and/or the Medvinsky. Since claim 22 is patentable at least by virtue of its dependency on independent claim 17, Applicants respectfully request that the rejection of claim 22 under 35 U.S.C. § 103(a) be withdrawn.

Claims 29 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Torigai in view of Gulcu. Applicants respectfully traverse this rejection for the reasons discussed below.

Claim 29 is believed to be allowable for at least the reasons set forth above regarding claim 17. The Gulcu reference fails to provide the teachings noted above as missing from the Torigai reference. Since claim 29 is patentable at least by virtue of its dependency on independent claim 17, Applicants respectfully request that the rejection of claim 29 under 35 U.S.C. § 103(a) be withdrawn.

CONCLUSION

In view of the above remarks and amendments, Applicants respectfully submit that each of the pending objections and rejections has been addressed and overcome, placing the present application in condition for allowance. A notice to that effect is respectfully requested. Further, the above remarks demonstrate the failings of the outstanding rejections, and are sufficient to overcome the rejections. However, these remarks are not intended to, nor need they, comprehensively address each and every reason for the patentability of the claimed subject matter over the applied prior art. Accordingly, Applicants do not contend that the claims are patentable solely on the basis of the particular claim elements discussed above.

Should there be any outstanding matters that need to be resolved in the present application, the Examiner is respectfully requested to contact the undersigned, at the telephone number below.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 08-0750 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17; particularly, extension of time fees.

Respectfully submitted,

HARNESS, DICKEY, & PIERCE, P.L.C.

By _____

John A. Castellano, Reg. No. 35,094

P.O. Box 8910
Reston, Virginia 20195
(703) 668-8000

JAC/DJC:clc